ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 31167—2023
代替 GB/T 31167—2014

信息安全技术　云计算服务安全指南

Information security technology—Security guidance for cloud computing services

2023-05-23 发布　　2023-12-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替GB/T 31167—2014《信息安全技术　云计算服务安全指南》，与GB/T 31167—2014相比，除结构调整和编辑性改动外，主要技术变化如下：

——更改了适用范围，由“政府部门”更改为“客户”（见第1章，见2014年版的第1章）；

——增加了对GB/T 32400—2015（见第3章）、GB/T 36325—2018（见7.3.3）、GB/T 37972—2019（见8.1）的规范性引用；

——增加并更改了部分术语（见第3章，2014年版的第3章）；

——增加了“缩略语”一章（见第4章）；

——删除了“云计算的概述”（见2014年版第4章）；

——增加了“云能力类型”和“云服务类别”的引用（全文）；

——将2014年版中的“5.2 云计算安全风险”作为资料性附录（见附录B）；

——将2014年版5.3内容作为“5.2.1 角色及职责”章节内容，并增加“云服务安全提供商”作为云计算服务安全管理的新角色（见5.2.1）；

——增加了“安全责任划分”的指导和示例（见5.2.2和附录A）；

——将“审查”更改为“评估”，与相关文件统一名称（全文）；

——删除了“效益评估”（见2014年版的6.2）；

——更改了2014年版“6.3 政府信息分类”的标题和内容（见6.2）；

——删除了“敏感信息”和“公开信息”相关的技术内容（见2014年版的6.3.2、6.3.3）；

——将标题“政府业务分类”更改为“业务分类”，扩大了业务范围（见6.3，见2014年版的6.4）；

——更改了业务分类中关键业务的条件（见6.3.4，见2014年版的6.4.4）；

——删除了“优先级确定”的内容（见2014年版的6.5）；

——更改了安全保护要求，提出了三级安全能力级别（见6.4，见2014年版的6.6）；

——更改了2014年版中的图3，增加了关键业务类型和高级安全能力（见图2）；

——删除了“6.7.1 概述”（见2014年版的6.7.1）；

——更改了2014年版中“6.7.2 服务模式”标题及内容，由服务模式划分控制范围更改为通过能力类型划分控制范围（见6.5.1）；

——更改了2014年版中的图4，将服务模式改为基本云服务能力类型（见图3）；

——增加了指导客户在迁移时对业务系统集成需求的考虑（见6.5.7，见2014年版的6.7.8）；

——更改了2014年版“6.7.9 数据的存储位置”的技术内容（见6.5.8）；

——更改了“7.1 云服务商安全能力要求”的内容，具体要求参见GB/T 31168—2023（见7.1，见2014年版的7.1）；

——删除了2014年版中的7.1.1至7.1.10章节（见2014年版7.1.1～7.1.10）；

——将2014年版本中7.2.2的内容合并至7.2（见7.2，见2014年版的7.2）；

——增加了服务水平协议的相关文件引用（见7.3.3，见2014年版的7.3.3）；

——更改了“8.1 概述”的内容，引入GB/T 37972—2019为云服务商和运行监管方开展云计算服务运行监管活动提供指导（见8.1，见2014年版的8.1）；

——更改了“8.2.1 概述”的内容，强调对云服务安全提供商的运行监管责任应由引入方承担（见

8.2.1，见 2014 年版的 8.2.1）；

——增加了运行监管中客户的相关责任（见 8.2.2，见 2014 年版的 8.2.2）；

——增加了重大变更的类型（见 8.4.3，见 2014 年版本的 8.4.2）；

——增加了安全事件的类型（见 8.4.4，见 2014 年版本的 8.4.3）；

——增加了“迁移原则”一节，用于指导客户在迁移数据时宜要求云服务商遵循的原则（见 9.2.1）；

——将 2014 年版中“9.2 确定移交范围”的内容更改为“9.2.2 移交范围”（见 9.2.2）；

——删除了“9.4 安全删除数据”中 c）条措施中的“3）存放敏感信息的介质清理后不能用于存放公开信息”（见 2014 年版的 9.4）；

——将 2014 年版中的“9.4 安全删除数据”中 c）条措施中的脚注作为 c）条措施中注（见 9.4）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：四川大学、中国科学技术大学、北京信息安全测评中心、华为技术有限公司、中国电子技术标准化研究院、北京天融信网络安全技术有限公司、国家信息技术安全研究中心、中国网络安全审查技术与认证中心、中国移动通信集团有限公司、陕西省信息化工程研究院、国家工业信息安全发展研究中心、浪潮云信息技术股份公司、深信服科技股份有限公司、中国信息安全测评中心（北京）、杭州安恒信息技术股份有限公司、中国电子科技集团公司第三十研究所、华信咨询设计研究院有限公司、中电长城网际系统应用有限公司、成都蜀道易信科技有限公司、新华三技术有限公司、腾讯云计算（北京）有限责任公司。

本文件主要起草人：陈兴蜀、周亚超、王启旭、闵京华、杨苗苗、罗永刚、张建军、杨建军、左晓栋、刘海峰、张滨、江为强、李媛、严敏瑞、王龑、王惠莅、张明天、张勇、卢夏、伍扬、陈雪鸿、史大为、柳彩云、张敏、邱勤、吴复伟、张晓菲、赵丹丹、望娅露、刘俊河、章建聪、陈静、万晓兰、马洪军、张格、董平、于乐、尹丽波、赵章界、朱毅、邱云翔、王永霞。

本文件及其所代替文件的历次版本发布情况为：

——2014 年首次发布为 GB/T 31167—2014；

——本次为第一次修订。

引　言

本文件与GB/T 31168—2023《信息安全技术　云计算服务安全能力要求》构成了云计算服务安全管理的基础文件。GB/T 31168—2023面向云服务商描述了为客户提供云计算服务时应具备的安全能力，本文件面向客户提出了采用云计算服务时的安全管理和技术措施。

本文件指导客户做好采用云计算服务的前期分析和规划，选择合适的云服务商与部署模式，对云计算服务进行运行监管，规避退出云计算服务或更换云服务商的安全风险。本文件指导客户在采用云计算服务的生命周期采取相应的安全技术和管理措施，保障数据和业务的安全，安全地使用云计算服务。

信息安全技术　云计算服务安全指南

1　范围

本文件提出了客户采用云计算服务的安全管理基本原则，给出了采用云计算服务的生命周期各阶段的安全管理和技术措施，提出了云计算服务安全管理原则和相关责任划分。

本文件适用于指导客户安全地采用云计算服务。

2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术　术语

GB/T 31168—2023　信息安全技术　云计算服务安全能力要求

GB/T 32400—2015　信息技术　云计算　概览与词汇

3　术语和定义

GB/T 25069—2022 和 GB/T 32400—2015 界定的以及下列术语和定义适用于本文件。

3.1

云计算　cloud computing

通过网络访问可扩展的、灵活的物理或虚拟共享资源池，并按需自助获取和管理资源的模式。

注：资源实例包括服务器、操作系统、网络、软件、应用和存储设备等。

［来源：ISO/IEC 17788：2014，3.2.5］

3.2

云服务　cloud service

云计算服务　cloud computing service

使用定义的接口，通过云计算（3.1）提供一种或多种资源的能力。

［来源：ISO/IEC 17788：2014，3.2.8，有修改］

3.3

参与方　party

一个或一组自然人或法人，无论其是否注册。

［来源：GB/T 32400—2015，3.1.6，有修改］

3.4

云服务提供者　cloud service provider

云服务商

提供云计算服务的参与方。

［来源：GB/T 32400—2015，3.2.15，有修改］